WE CLAIM:

1. A method of conducting a transaction by a purchaser over a communications network, comprising:

(a) assigning to said purchaser a first payment account number having a status which changes over time;

(b) providing a second payment account number associated with said first payment account number, said second payment account number not being a transaction number and having an encryption key assigned thereto;

(c) requesting authorization for payment of said transaction with said second payment account number and not said first payment account number;

(d) identifying said purchaser's first payment account number in response to said authorization request; and

(e) responding to said authorization request based upon said status of said first payment account number at the time of the transaction.

2. The method of claim 1, wherein said authorization request includes a cryptographic code based on said encryption key, and wherein said response to said authorization request is further based on said cryptographic code.

3. The method of claim 2, wherein said status is a function of the credit balance available for use by said purchaser, which credit balance changes over time as a result of the purchases made by the purchaser.

4. A method of conducting a transaction by a purchaser over a communications network, comprising:

(a) assigning to said purchaser a first payment account number having a status which changes over time;

(b) providing said purchaser with a secure payment application which includes a cryptographic key that is unique to said account number and a pseudo account number having the same length as and associated with said first payment account number;

(c) providing said purchaser with merchant data based on the transaction;

(d) generating a message authentication code as a function of at least said merchant data and said cryptographic key;

(e) providing said merchant said pseudo account number and said message authentication code and not said first payment account number;

(f) verifying that said merchant data is the correct data for the transaction;

(g) requesting an authorization for payment of said transaction, said authorization request not including said first payment account number but including said pseudo account number;

(h) recognizing said pseudo account number and cryptographically processing said pseudo account number to produce said first payment account number; and

(i) responding to said authorization request based on the status of said first payment account number, and passing said response back without transmission of said first payment account number.

5. The method of claim 4 wherein said pseudo account number is indicated to be different from said first payment account number by a special identifier within the pseudo account number.

6. The method of claim 4 wherein said pseudo account number is indicated to be such by data within a transaction record.

7. The method of claim 4 wherein said cryptographic key is a secret key.

8. The method of claim 4 wherein said cryptographic key is a private key and said secure payment application further includes a card-unique certificate for the corresponding public key and said message authentication code comprises a digital signature generated by said secure payment application.

9. The method of claim 4 wherein said pseudo account number is obtained by encrypting the associated first payment account number utilizing DESX methodology.

10. The method of claim 4 wherein said pseudo account number is converted back into its associated first payment account number utilizing DEA with a double-length key.